

David Hilton Wise, Esq.  
Nevada Bar No. 11014  
**WISE LAW FIRM, PLC**  
421 Court Street  
Reno, Nevada 89501  
Tel: (775) 329-1766  
Fax: (775) 329-2432  
Email: dwise@wiselaw.pro

M. Anderson Berry (*pro hac vice forthcoming*)  
Gregory Haroutunian (*pro hac vice forthcoming*)  
**CLAYEO C. ARNOLD,**  
**A PROFESSIONAL CORP.**  
865 Howe Avenue  
Sacramento, CA 95825  
Telephone: (916) 777-7777  
Facsimile: (916) 924-1829  
aberry@justice4you.com  
gharoutunian@justice4you.com

*Attorneys for Plaintiff and the Class*

**UNITED STATES DISTRICT COURT**  
**DISTRICT OF NEVADA**

GARY LESTER, individually and on behalf of all  
others similarly situated,

Plaintiff,

v.

DON LAUGHLIN's RIVERSIDE RESORT  
HOTEL & CASINO, d/b/a RIVERSIDE RESORT  
& CASINO,

Defendant.

Case No. 2:24-cv-1760

**CLASS ACTION COMPLAINT**

Plaintiff Gary Lester ("Plaintiff" or "Plaintiff Lester"), individually and on behalf of all others similarly situated, brings this action against Defendant Don Laughlin's Riverside Resort Hotel & Casino d/b/a Riverside Resort Hotel & Casino ("Riverside Resort" or "Defendant"), to obtain damages,

1 restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the  
2 following allegations upon information and belief, except as to his own actions, the investigation of his  
3 counsel, and the facts that are a matter of public record:  
4

5  
6 **NATURE OF THE ACTION**

7 1. This is a data breach class action brought on behalf of consumers whose sensitive personal  
8 information was stolen by cybercriminals in a massive cyber-attack at Riverside Resort on or about July  
9 25, 2024 (the “Data Breach”). The Data Breach reportedly involved at least 55,155 individuals.  
10

11 2. Information stolen in the Data Breach included individuals’ sensitive information,  
12 including at least, full names and Social Security numbers (collectively, the “Private Information” or  
13 “PII”). Plaintiff and Class Members face an ongoing and lifetime risk of identity theft, which is heightened  
14 by the exposure of their Social Security numbers.

15 3. On or around September 5, 2024, Plaintiff received a letter from Defendant (the “Notice of  
16 Data Breach”), which stated the following:

17 On July 25, 2024, Riverside learned of suspicious activity in its environment. Upon  
18 discovery, Riverside immediately engaged forensic specialists in cybersecurity and data  
19 privacy to investigate further. Through this investigation, Riverside determined that an  
20 unauthorized third party potentially accessed and acquired certain files during this incident.  
21 Riverside then performed an extensive and comprehensive review of the data to identify what  
22 personal information may have been impacted in this incident.

23 4. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses  
24 in the form of loss of the value of their private and confidential information, loss of the benefit of their  
25 contractual bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or  
26 mitigate the effects of the attack.  
27  
28

1           5.       Plaintiff's and Class Members' sensitive personal information—which was entrusted to  
2 Defendant, their officials, and agents—was compromised, unlawfully accessed, and stolen due to the Data  
3 Breach.

4           6.       Plaintiff brings this class action lawsuit on behalf of those similarly situated to address  
5 Defendant's inadequate safeguarding of Class Members' Private Information that it collected and  
6 maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members  
7 that their information had been subject to the unauthorized access of an unknown third party and precisely  
8 what specific type of information was accessed.  
9

10           7.       Defendant maintained the Private Information in a reckless manner. In particular, the  
11 Private Information was maintained on Defendant's computer network in a condition vulnerable to  
12 cyberattacks of this type.  
13

14           8.       Upon information and belief, the mechanism of the cyber-attack and potential for improper  
15 disclosure of Plaintiff's and Class Members' Private Information was a known and foreseeable risk to  
16 Defendant, and Defendant was on notice that failing to take steps necessary to secure the Private  
17 Information from those risks left that property in a dangerous condition.  
18

19           9.       Because of the Data Breach, Plaintiff and Class Members suffered injury and damages in  
20 the form of theft and misuse of their Private Information.

21           10.       In addition, Plaintiff's and Class Members' identities are now at risk because of  
22 Defendant's negligent conduct since the Private Information that Defendant collected and maintained is  
23 now in the hands of data thieves.  
24

25           11.       Armed with the Private Information accessed in a cybersecurity incident, data thieves can  
26 commit a variety of crimes including, for example, opening new financial accounts under Class Members'  
27 names, taking out loans in Class Members' names, using Class Members' names to obtain medical  
28 services, using Class Members' information to obtain government benefits, filing fraudulent tax returns

1 using Class Members' information, obtaining driver's licenses in Class Members' names but with another  
2 person's photograph, and giving false information to police during an arrest.

3 12. As a further result of the Data Breach, Plaintiff and Class Members have been exposed to  
4 a substantial and present risk of fraud and identity theft. Plaintiff and Class Members must now and in the  
5 future closely monitor their financial accounts to guard against identity theft.  
6

7 13. Plaintiff and Class Members have and may also incur out-of-pocket costs for, for example,  
8 purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter  
9 and detect identity theft.

10 14. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have  
11 suffered and will continue to suffer damages and economic losses in the form of: the loss of time needed  
12 to: take appropriate measures to monitor potential identity fraud and avoid unauthorized charges; change  
13 their usernames and passwords on their accounts; monitor, correct, and resolve unauthorized debits,  
14 charges, and fees charged against their accounts; and deal with spam messages and e-mails received as a  
15 result of the Data Breach. Plaintiff and Class Members have likewise suffered and will continue to suffer  
16 an invasion of their property interest in their own Private Information such that they are entitled to  
17 damages for unauthorized access to and misuse of their Private Information from Defendant. Further,  
18 Plaintiff and Class Members presently and will continue to suffer from damages associated with the  
19 unauthorized use and misuse of their Private Information as thieves will continue to use the stolen  
20 information to obtain money and credit in their name for several years.  
21

22 15. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated  
23 individuals whose Private Information was accessed and/or removed from the network during the Data  
24 Breach.  
25

26 16. Plaintiff seeks remedies including, but not limited to, compensatory damages,  
27 reimbursement of out-of-pocket costs, and injunctive relief, including improvements to Defendant's data  
28

1 security systems, future annual audits, and adequate credit monitoring and identity restoration services  
2 funded by Defendant.

3 17. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful  
4 conduct.  
5

6  
7 **PARTIES**

8 18. Plaintiff Gary Lester is a resident and citizen of Arizona. Plaintiff Lester is acting on his  
9 own behalf and on behalf of others similarly situated. Riverside Resort obtained and continues to maintain  
10 Plaintiff Lester's Private Information and has a legal duty and obligation to protect that Private  
11 Information from unauthorized access and disclosure. Plaintiff Lester would not have entrusted his Private  
12 Information to Riverside Resort had he known that Riverside Resort would fail to maintain adequate data  
13 security. Plaintiff Lester's Private Information was compromised and disclosed as a result of the Data  
14 Breach.  
15

16 19. Defendant Riverside Resort is a Nevada corporation with its principal place of business at  
17 1650 S Casino Drive, Laughlin, Nevada, 89029.  
18

19 **JURISDICTION AND VENUE**

20 20. This Court has subject matter jurisdiction over this action under the Class Action Fairness  
21 Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the  
22 individual Class Members exceed the sum or value of \$5,000,000 exclusive of interest and costs, and,  
23 upon information and belief, members of the proposed Class are citizens of states different from  
24 Defendant.  
25

26 21. This Court has jurisdiction over Defendant through its business operations in this District,  
27 the specific nature of which occurs in this District. Defendant intentionally avails itself of the markets  
28 within this District to render the exercise of jurisdiction by this Court just and proper.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District.

### **FACTUAL ALLEGATIONS**

#### **Defendant's Business**

23. Defendant Don Laughlin's Riverside Resort Hotel & Casino is a well-known resort located in Laughlin, Nevada, and this is the primary and only location of the resort. Founded in 1966 by Don Laughlin, Defendant's resort attracts 5 million visitors annually.<sup>1</sup>

24. Defendant's resort offers a comprehensive experience with over 1,400 rooms, diverse dining options, and a variety of entertainment, including movie theater, live shows, as well as casino features.<sup>2</sup>

25. In the ordinary course of doing business, Defendant requires customers to provide sensitive, personal, and private information, including but not limited to customers' names, driver's license information, addresses, phone numbers, debit or credit card information, and Social Security numbers.

26. As a condition of transacting with Defendant, Plaintiff was required to disclose some or all of the Private Information listed above.<sup>3</sup>

---

<sup>1</sup> See <https://www.riversideresort.com/don-laughlin-history-founder-riverside-resort-casino/> (Last accessed on September 16, 2024).

<sup>2</sup> See <https://www.riversideresort.com/don-laughlin-history-founder-riverside-resort-casino/about-us/> (Last accessed on September 16, 2024).

<sup>3</sup> *Privacy Policy*, <https://www.riversidecasinoandresort.com/privacy.html> (Last accessed on September 16, 2024).

1           27. On information and belief, in the course of collecting Private Information from consumers,  
2 including Plaintiff, Defendant promised to provide confidentiality and adequate security for customer data  
3 through its applicable privacy policy and through other disclosures.<sup>4</sup>  
4  
5  
6

7           **The Cyber-Attack and Data Breach**

8           28. On July 25, 2024, Defendant detected suspicious activity in its system. Through its  
9 investigation, Defendant confirmed that “an authorized third party potentially accessed and acquired  
10 certain files”.<sup>5</sup>  
11

12           29. According to Defendant, its investigation identified the individuals whose PII was  
13 compromised on August 9, 2024. However, Defendant delayed almost another month to notify the victims  
14 and the Attorney General Offices in Maine and California on September 5, 2024.

15           30. According to Defendant, hackers accessed and obtained consumers’ Private Information,  
16 which included, at least, full names and Social Security numbers.<sup>6</sup>  
17

18           31. Up until today, Defendant still has not disclosed critical details regarding the Data Breach,  
19 such as the reasons behind it, the hackers’ identity, the measures they have taken to remediate the situation,  
20 whether all victims were customers or employees.

21           32. The cyber-attack was expressly designed and targeted to gain access to private and  
22 confidential data, including (among other things) the personal information, or PII, of Defendant’s  
23 customers and clients, including Plaintiff and Class Members, and possibly employees. Evidence of this  
24  
25

---

26 <sup>4</sup> *Id.*

27 <sup>5</sup> Office of the Maine Attorney General, Data Breach Notifications,  
28 <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/ab5c465c-1b23-4a88-9a62-253cad91b22b.html>  
(last accessed on September 16, 2024).

<sup>6</sup> *Id.*

1 specific targeting of Private Information is the fact that, according to Defendant's own forensic  
2 investigation, an "unauthorized actor potentially accessed and acquired" the Private Information.<sup>7</sup>

3 33. Defendant notified impacted individuals on or about September 5, 2024.<sup>8</sup>

4 34. As a result of Defendant's delay in providing notice, the risk of harm to Plaintiff and Class  
5 Members has increased. Consumer Reports has noted: "One thing that does matter is hearing about a data  
6 breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It  
7 can prompt them to change passwords and freeze credit reports... If consumers don't know about a breach  
8 because it wasn't reported, they can't take action to protect themselves."<sup>9</sup>

9 35. Defendant also failed to encrypt the PII stored on its server, evidenced by the fact that  
10 hackers were able to steal the Private Information in a readable form.

11 36. Defendant acknowledges that Plaintiff and Class Members face a substantial and present  
12 risk of identity theft because it is actively encouraging them to "remain vigilant against vigilant against  
13 incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports  
14 for suspicious or unauthorized activity."<sup>10</sup>

15 37. Based on the Notice of Data Breach letter he received, Plaintiff believes his Private  
16 Information was stolen from Defendant's networks as a result of the Data Breach.

17 38. Further, the acquisition of the Private Information from Defendant's system demonstrates  
18 that this cyberattack was targeted.

19  
20  
21  
22  
23  
24  
25 <sup>7</sup> *Id.*

26 <sup>8</sup> Plaintiff's Notice of Data Breach is dated September 5, 2024.

27 <sup>9</sup> *The Data Breach Next Door*, Consumer Reports, Jan. 31, 2019, available at:  
28 <https://www.consumerreports.org/data-theft/the-data-breach-next-door/> (last accessed on September 16, 2024).

<sup>10</sup> See Notice of Data Breach, *supra*, at <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/ab5c465c-1b23-4a88-9a62-253cad91b22b.html>.

1           39. Defendant had obligations created by contract, industry standards, common law, and  
2 representations made to Plaintiff and Class Members, to keep their Private Information confidential and  
3 to protect it from unauthorized access and disclosure.

4           40. Plaintiff and Class Members provided their Private Information to Defendant with the  
5 reasonable expectation and mutual understanding that Defendant would comply with their obligations to  
6 keep such information confidential and secure from unauthorized access.

7           41. Defendant's data security obligations were particularly important given the substantial  
8 increase in cyber-attacks and/or data breaches in the restaurant services industry preceding the date of the  
9 breach.

10           42. Data breaches, including those perpetrated against the restaurant services sector of the  
11 economy, have become widespread. In fact, a similar data breach occurred recently involving another  
12 casino/restaurant in Nevada, where the defendant is facing a similar class action lawsuit in this District  
13 Court.<sup>11</sup>

14           43. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455  
15 sensitive records being exposed, a 17% increase from 2018.<sup>12</sup>

16           44. According to Bluefin, "[t]he restaurant and hospitality industries have been hit particularly  
17 hard by data breaches, with hotel brands, restaurants and establishments targeted by hackers in 2019."<sup>13</sup>  
18  
19  
20  
21  
22  
23  
24

25 <sup>11</sup> [https://databreaches.net/2021/09/06/nevada-restaurant-services-inc-provides-notice-of-data-privacy-](https://databreaches.net/2021/09/06/nevada-restaurant-services-inc-provides-notice-of-data-privacy-event/)  
26 [event/](https://databreaches.net/2021/09/06/nevada-restaurant-services-inc-provides-notice-of-data-privacy-event/) (last visited on September 16, 2024).

27 <sup>12</sup> [https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020\\_ITRC\\_2019-End-of-Year-](https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf)  
28 [Data-Breach-Report\\_FINAL\\_Highres-Appendix.pdf](https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf) (last visited on September 16, 2024).

<sup>13</sup> [https://www.bluefin.com/bluefin-news/the-rise-in-restaurant-data-breaches-and-the-need-to-devalue-](https://www.bluefin.com/bluefin-news/the-rise-in-restaurant-data-breaches-and-the-need-to-devalue-consumer-data/)  
consumer-data/ (last visited on September 16, 2024).

1           45. Another report says that the “companies in the food and beverage industry are the most at  
2 risk from cybercriminals.”<sup>14</sup>

3           46. According to Kroll, “data-breach notifications in the food and beverage industry shot up  
4 1,300% in 2020.”<sup>15</sup>

5           47. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so  
6 notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning  
7 to potential targets, so they are aware of, and prepared for, a potential attack. Therefore, the increase in  
8 such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the  
9 public and to anyone in Defendant’s industry, including Defendant.  
10

11           **Defendant Fails to Comply with FTC Guidelines**

12           48. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses  
13 which highlight the importance of implementing reasonable data security practices. According to the FTC,  
14 the need for data security should be factored into all business decision-making.  
15

16           49. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for*  
17 *Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses  
18 should protect the personal customer information that they keep; properly dispose of personal information  
19 that is no longer needed; encrypt information stored on computer networks; understand their network’s  
20 vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend  
21 that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all  
22  
23  
24  
25

26 <sup>14</sup> [https://www.industryweek.com/finance/article/21959093/food-and-beverage-industry-most-at-risk-](https://www.industryweek.com/finance/article/21959093/food-and-beverage-industry-most-at-risk-for-cyber-attack)  
27 [for-cyber-attack](https://www.industryweek.com/finance/article/21959093/food-and-beverage-industry-most-at-risk-for-cyber-attack) (last visited on September 16, 2024).

28 <sup>15</sup> [https://www.darkreading.com/attacks-breaches/data-breaches-surge-in-food-and-beverage-other-](https://www.darkreading.com/attacks-breaches/data-breaches-surge-in-food-and-beverage-other-industries/d/d-id/1341336)  
[industries/d/d-id/1341336](https://www.darkreading.com/attacks-breaches/data-breaches-surge-in-food-and-beverage-other-industries/d/d-id/1341336) (last visited on September 16, 2024).

1 incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts  
2 of data being transmitted from the system; and have a response plan ready in the event of a breach.

3 50. The FTC further recommends that companies not maintain PII longer than is needed for  
4 authorization of a transaction; limit access to sensitive data; require complex passwords to be used on  
5 networks; use industry-tested methods for security; monitor for suspicious activity on the network; and  
6 verify that third-party service providers have implemented reasonable security measures.

7 51. The FTC has brought enforcement actions against businesses for failing to protect customer  
8 data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to  
9 protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited  
10 by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these  
11 actions further clarify the measures businesses must take to meet their data security obligations.

12 52. These enforcement actions include actions against healthcare providers like Defendant.  
13 *See, e.g., In the Matter of LabMD, Inc., A Corp, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215,*  
14 *at \*32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices were*  
15 *unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”).*

16 53. Defendant failed to properly implement basic data security practices, and its failure to  
17 employ reasonable and appropriate measures to protect against unauthorized access to customer PII  
18 constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

19 54. Defendant was at all times fully aware of their obligation to protect the PII of customers.  
20 Defendant were also aware of the significant repercussions that would result from its failure to do so.

21 **Defendant Failed to Comply with Industry Standards**

22 55. A number of industry and national best practices have been published and should have  
23 been used as a go-to resource and authoritative guide when developing Defendant’s cybersecurity  
24 practices.  
25  
26  
27  
28

1           56. Best cybersecurity practices that are standard in Defendant's industry include installing  
2 appropriate malware detection software; monitoring and limiting the network ports; protecting web  
3 browsers and email management systems; setting up network systems such as firewalls, switches and  
4 routers; monitoring and protection of physical security systems; protection against any possible  
5 communication system; training staff regarding critical points.

7           57. Upon information and belief, Defendant failed to meet the minimum standards of the  
8 following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without  
9 limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,  
10 PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet  
11 Security's Critical Security Controls (CIS CSC), which are established standards in reasonable  
12 cybersecurity readiness.

14           58. These foregoing frameworks are existing and applicable industry standards in Defendant's  
15 industry. Defendant knew it was a target for hackers. Despite understanding the risks and consequences  
16 of inadequate data security, Defendant failed to comply with these accepted standards, thereby opening  
17 the door to the cyber-attack and causing the Data Breach.

18  
19           **Defendant's Breach**

20           59. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise  
21 negligent and reckless because it failed to properly maintain and safeguard its computer systems,  
22 networks, and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or  
23 omissions:

- 24           a. Failing to maintain an adequate data security system to reduce the risk of data breaches and  
25 cyber-attacks;  
26  
27           b. Failing to adequately protect customers' Private Information;

- c. Failing to properly monitor its own data security systems for existing intrusions, encryptions, brute-force attempts, and clearing of event logs;
- d. Failing to apply all available security updates;
- e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;
- f. Failing to practice the principle of least-privilege and maintain credential hygiene;
- g. Failing to avoid the use of domain-wide, admin-level service accounts;
- h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords, and;
- i. Failing to properly train and supervise employees in the proper handling of inbound emails.

60. As the result of computer systems in dire need of security upgrading and inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

61. Accordingly, as outlined below, Plaintiff and Class Members now face a substantial, increased, and present risk of fraud and identity theft.

62. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant because of its inadequate data security practices for which they gave good and valuable consideration.

**Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft**

63. Defendant was well aware that the Private Information it collects is highly sensitive, and of significant value to those who would use it for wrongful purposes, like the operators who perpetrated this cyber-attack.

1           64.     The United States Government Accountability Office released a report in 2007 regarding  
2 data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs  
3 and time to repair the damage to their good name and credit record.”<sup>16</sup>

4  
5           65.     That is because any victim of a data breach is exposed to serious ramifications  
6 regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable  
7 information is to monetize it.

8           66.     They do this by selling the spoils of their cyberattacks on the black market to identity  
9 thieves who desire to extort and harass victims, take over victims’ identities in order to engage in  
10 illegal financial transactions under the victims’ names. Because a person’s identity is akin to a puzzle,  
11 the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief  
12 to take on the victim’s identity, or otherwise harass or track the victim.

13  
14           67.     For example, armed with just a name and date of birth, a data thief can use a hacking  
15 technique referred to as “social engineering” to obtain even more information about a victim’s  
16 identity, such as a person’s login credentials or Social Security number.

17           68.     Social engineering is a form of hacking whereby a data thief uses previously acquired  
18 information to manipulate individuals into disclosing additional confidential or personal information  
19 through means such as spam phone calls and text messages or phishing emails.

20  
21           69.     The FTC recommends that identity theft victims take several steps to protect their personal  
22 and financial information after a data breach, including contacting one of the credit bureaus to place a  
23 fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity),  
24  
25  
26  
27

28 <sup>16</sup> See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited on Feb. 21, 2023) (“GAO Report”).

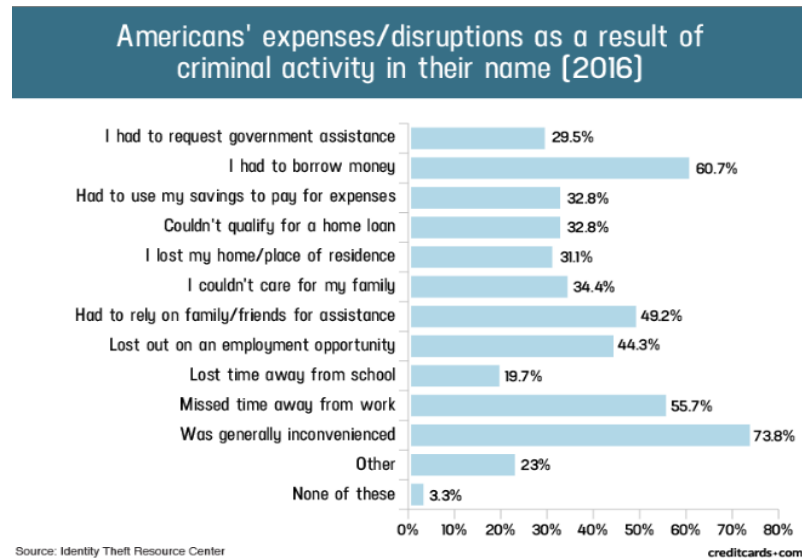
reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.<sup>17</sup>

70. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

71. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

72. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

73. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:<sup>18</sup>



<sup>17</sup> See <https://www.identitytheft.gov/Steps> (last visited on September 18, 2024).

<sup>18</sup> See Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020), available at: <https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/> (last visited on September 18, 2024).

1           74.     What’s more, theft of Private Information is also gravely serious. PII is a valuable property  
2 right.<sup>19</sup>

3           75.     Its value is axiomatic, considering the value of Big Data in corporate America and the  
4 consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis  
5 illustrates beyond doubt that Private Information has considerable market value.  
6

7           76.     It must also be noted there may be a substantial time lag – measured in years – between  
8 when harm occurs versus when it is discovered, and also between when Private Information and/or  
9 financial information is stolen and when it is used.

10          77.     According to the U.S. Government Accountability Office, which conducted a study  
11 regarding data breaches:

12                   [L]aw enforcement officials told us that in some cases, stolen data may be held  
13 for up to a year or more before being used to commit identity theft. Further,  
14 once stolen data have been sold or posted on the Web, fraudulent use of that  
15 information may continue for years. As a result, studies that attempt to measure  
16 the harm resulting from data breaches cannot necessarily rule out all future  
harm.

17 *See* GAO Report, at p. 29.

18          78.     Private Information and financial information are such valuable commodities to identity  
19 thieves that once the information has been compromised, criminals often trade the information on the  
20 “cyber black-market” for years.

21          79.     There is a strong probability that entire batches of stolen information have been  
22 dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and  
23 Class Members are at a substantial and immediate present risk of fraud and identity theft that will  
24 continue for many years.  
25

26  
27 <sup>19</sup> *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable  
28 Information (“PII”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at \*3-4 (2009) (“PII,  
which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to  
the value of traditional financial assets.”) (citations omitted).

1           80.     Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical  
2 accounts for many years to come.

3           81.     Sensitive Private Information can sell for as much as \$363 according to the Infosec  
4 Institute.

5           82.     PII is particularly valuable because criminals can use it to target victims with frauds and  
6 scams.

7           83.     Once PII is stolen, fraudulent use of that information and damage to victims may continue  
8 for years.

9           84.     The PII of consumers remains of high value to criminals, as evidenced by the prices they  
10 will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For  
11 example, personal information can be sold at a price ranging from \$40 to \$200.

12           85.     Social Security numbers are among the worst kind of personal information to have stolen  
13 because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The  
14 Social Security Administration stresses that the loss of an individual's Social Security number, as is the  
15 case here, can lead to identity theft and extensive financial fraud.

16           86.     For example, the Social Security Administration has warned that identity thieves can use  
17 an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected  
18 until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also  
19 make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a  
20 job using a false identity.

21           87.     Each of these fraudulent activities is difficult to detect. An individual may not know that  
22 his or her Social Security Number was used to file for unemployment benefits until law enforcement  
23 notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered  
24 only when an individual's authentic tax return is rejected.

1 88. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

2 89. An individual cannot obtain a new Social Security number without significant paperwork  
3 and evidence of actual misuse. Even then, a new Social Security number may not be effective, as “[t]he  
4 credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old  
5 bad information is quickly inherited into the new Social Security number.”<sup>20</sup>  
6

7 90. This data, as one would expect, demands a much higher price on the black market. Martin  
8 Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information,  
9 personally identifiable information and Social Security Numbers are worth more than 10x on the black  
10 market.”<sup>21</sup>  
11

12 91. At all relevant times, Defendant knew or reasonably should have known these risks, the  
13 importance of safeguarding Private Information, and the foreseeable consequences if its data security  
14 systems were breached and strengthened its data systems accordingly. Defendant was put on notice of the  
15 substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.  
16

17 **Plaintiff’s and Class Members’ Damages**

18 92. To date, Defendant has done absolutely nothing to provide Plaintiff and Class Members  
19 with relief for the damages they have suffered as a result of the cyber-attack and data breach, including,  
20 but not limited to, the costs and loss of time they incurred because of the cyber-attack. The complimentary  
21 credit monitoring service offered by Defendant is wholly inadequate as the services are only offered for  
22  
23  
24

25 <sup>20</sup> *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9,  
26 2015, available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited on September 18, 2024).

27 <sup>21</sup> *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*,  
28 NetWorldWorld, Tim Greene, Feb. 6, 2015, available at: <https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited on September 18, 2024).

1 12 months, and it places the burden squarely on Plaintiff and Class Members by requiring them to expend  
2 time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

3 93. Moreover, Defendant entirely fails to provide any compensation for the unauthorized  
4 release and disclosure of Plaintiff's and Class Members' PII.

5 94. Plaintiff and Class Members have been damaged by the compromise of their Private  
6 Information in the Data Breach.

7  
8 **Plaintiff Lester's Experience**

9 95. Plaintiff Lester has been a loyal customer of Riverside Resort for over 15 years. Upon  
10 every visit, Riverside Resort required Plaintiff to provide his name, Social Security number, driver's  
11 license information, address, phone numbers, and some financial information for payment and for  
12 membership at its players club. The last time he visited Riverside Resort was in September 2024.

13 96. On or about September 5, 2024, Plaintiff Lester received notice from Riverside Resort that  
14 his Private Information had been improperly accessed during a cybersecurity incident that was detected  
15 by Defendant on July 25, 2024. Riverside Resort notified Plaintiff and Class members that it "determined  
16 that an unauthorized third party potentially accessed and acquired certain files during this incident," and  
17 that the information compromised included Plaintiff's "[n]ame and Social Security number." There is no  
18 indication from Defendant that the PII was encrypted or redacted in any way.

19 97. As a result of the Data Breach, Plaintiff Lester has encountered a significant uptick of spam  
20 communications, including unsolicited emails, calls, and text messages.

21 98. Plaintiff Lester made reasonable efforts to mitigate the impact of the Data Breach after  
22 receiving the data breach notification, including but not limited to: researching the Data Breach; reviewing  
23 credit reports and financial account statements for any indications of actual or attempted identity theft or  
24 fraud; enrolling in the credit monitoring and identity theft protection services offered by Riverside Resort;  
25 actively checking his credit monitoring service; and blocking unsolicited spam communications. In less  
26  
27  
28

1 than two weeks since being notified, Plaintiff has already spent at least 6 hours dealing with the Data  
2 Breach—valuable time that he otherwise would have spent on other activities, including recreation.

3 99. Plaintiff and Class Members will need identity theft protection services and credit  
4 monitoring services for their respective lifetimes, considering the immutable nature of the PII at issue,  
5 especially their Social Security numbers.  
6

7 100. As a result of the Data Breach, Plaintiff Lester has suffered emotional distress as a result  
8 of the release of his Private Information, which he believed would be protected from unauthorized access  
9 and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private  
10 Information for purposes of identity theft and fraud. Plaintiff Lester is very concerned about identity theft  
11 and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.  
12

13 101. Plaintiff Lester suffered actual injury from having his Private Information compromised as  
14 a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his  
15 Private Information, a form of property that Riverside Resort obtained from Plaintiff Lester; (b) violation  
16 of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of  
17 identity theft and fraud.  
18

19 102. As a result of the Data Breach, Plaintiff Lester anticipates spending considerable time and  
20 money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of  
21 the Data Breach, Plaintiff Lester will continue to be at substantial and immediate risk of identity theft and  
22 fraud for years to come.

23 103. Simply put, Plaintiff and Class Members now face substantial risk of out-of-pocket fraud  
24 losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility  
25 bills opened in their names, credit card fraud, and similar identity theft.  
26  
27  
28

1           104. Plaintiff and Class Members have been and face a substantial risk of being targeted in the  
2 future, subjected to phishing, data intrusion, and other illegal actions based on their Private Information  
3 as potential fraudsters could use that information to target such schemes more effectively.

4           105. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures  
5 such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly  
6 related to the cyber-attack.

7           106. Plaintiff and Class Members also suffered a loss of value of their Private Information when  
8 it was acquired by cyber thieves in the cyber-attack. Numerous courts have recognized the propriety of  
9 loss of value damages in related cases.

10           107. Class Members were also damaged via benefit-of-the-bargain damages, in that they  
11 overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of  
12 the price Class Members paid to Defendant was intended to be used by Defendant to fund adequate  
13 security of Defendant's computer property and Plaintiff's and Class Members' Private Information. Thus,  
14 Plaintiff and the Class Members did not get what they paid for.

15           108. Plaintiff and Class Members have spent and will continue to spend significant amounts of  
16 time to monitor their financial and medical accounts and records for misuse.

17           109. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of  
18 the cyber-attack. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and  
19 the value of their time reasonably incurred to remedy or mitigate the effects of the cyber-attack relating  
20 to:

- 21           a. Finding fraudulent charges;  
22           b. Canceling and reissuing credit and debit cards;  
23           c. Purchasing credit monitoring and identity theft prevention;  
24           d. Addressing their inability to withdraw funds linked to compromised accounts;

- e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- f. Placing “freezes” and “alerts” with credit reporting agencies;
- g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
- h. Contacting financial institutions and closing or modifying financial accounts;
- i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;
- j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be canceled; and
- k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

110. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

111. Further, as a result of Defendant’s conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person’s life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

112. Plaintiff and Class Members were also injured and damaged by the delayed notice of this data breach, as it exacerbated the substantial and present risk of harm by leaving Plaintiff and Class Members without the knowledge that would have enabled them to take proactive steps to protect themselves.

113. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at a present and definitely increased risk of future harm.

### **CLASS ACTION ALLEGATIONS**

114. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

115. Plaintiff brings this action individually and on behalf of all other persons similarly situated pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5).

116. Plaintiff proposes the following Class definitions, subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff brings this action and seeks certification of the following Class:

National Class: All persons whose PII was compromised as a result of the cyber-attack that Riverside Resort discovered on or about July 25, 2024, and who were sent the Notice of Data Breach.

Excluded from the Class are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

117. Plaintiff reserves the right to amend the definitions of the Class or add a Class if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

118. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

1           119. Numerosity. The members of the Classes are so numerous that joinder of all of them is  
2 impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on  
3 information and belief, the Class consists of thousands of Defendant's customers and policyholders whose  
4 data was compromised in the cyber-attack and data breach.

5  
6           120. Commonality. There are questions of law and fact common to the Classes, which  
7 predominate over any questions affecting only individual Class Members. These common questions of  
8 law and fact include, without limitation:

- 9           a) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and  
10 Class Members' Private Information;
- 11           b) Whether Defendant failed to implement and maintain reasonable security  
12 procedures and practices appropriate to the nature and scope of the information  
13 compromised in the cyber-attack;
- 14           c) Whether Defendant's data security systems prior to and during the cyber-attack  
15 complied with applicable data security laws and regulations;
- 16           d) Whether Defendant's data security systems prior to and during the cyber-attack  
17 were consistent with industry standards;
- 18           e) Whether Defendant owed a duty to Class Members to safeguard their Private  
19 Information;
- 20           f) Whether Defendant breached its duty to Class Members to safeguard their Private  
21 Information;
- 22           g) Whether computer hackers obtained Class Members' Private Information in the  
23 cyber-attack;
- 24           h) Whether Defendant knew or should have known that its data security systems and  
25 monitoring processes were deficient;
- 26  
27  
28

- i) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j) Whether Defendant owed a duty to provide Plaintiff and Class Members notice of this data breach, and whether Defendant breached that duty;
- k) Whether Defendant's conduct was negligent;
- l) Whether Defendant's acts, inactions, and practices complained of herein amount to an invasion of privacy;
- m) Whether Defendant's actions violated federal law; and
- n) Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief.

121. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the cyber-attack.

122. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff's Counsel are competent and experienced in litigating class actions.

123. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

124. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would likely find that the cost of litigating their individual claim is prohibitively high and would, therefore, have no

1 effective remedy. The prosecution of separate actions by individual class members would create a risk of  
2 inconsistent or varying adjudications with respect to individual class members, which would establish  
3 incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action  
4 presents far fewer management difficulties, conserves judicial resources and the parties' resources, and  
5 protects the rights of each class member.  
6

7 125. Defendant has acted on grounds that apply generally to the Classes as a whole, so that class  
8 certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.  
9

### 10 **CAUSES OF ACTION**

#### 11 **COUNT I** 12 **NEGLIGENCE**

#### 13 **(On Behalf of Plaintiff and All Class Members)**

14 126. Plaintiff and the Class re-allege and incorporate by reference herein all of the  
15 allegations contained in paragraphs 1 through 125.

16 127. Defendant required Plaintiff and Class Members to submit non-public personal information  
17 in order to obtain services, products and/or otherwise transact with Defendant.

18 128. By collecting and storing this data in its computer property, and sharing it and using it for  
19 commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its  
20 computer property—and Class Members' Private Information held within it—to prevent disclosure of the  
21 information, and to safeguard the information from theft. Defendant's duty included a responsibility to  
22 implement processes by which they could detect a breach of its security systems in a reasonably  
23 expeditious period of time and to give prompt notice to those affected in the case of a data breach.  
24

25 129. Defendant owed a duty of care to Plaintiff and Class Members to provide data security  
26 consistent with industry standards and other requirements discussed herein, and to ensure that its systems  
27 and networks, and the personnel responsible for them, adequately protected the Private Information.  
28

1           130. Defendant's duty of care to use reasonable security measures arose Defendant were in a  
2 position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class  
3 Members from a data breach.

4           131. In addition, Defendant had a duty to employ reasonable security measures under Section 5  
5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting  
6 commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use  
7 reasonable measures to protect confidential data.  
8

9           132. Defendant breached its duties, and thus was negligent, by failing to use reasonable  
10 measures to protect Class Members' Private Information. The specific negligent acts and omissions  
11 committed by Defendant include, but are not limited to, the following:  
12

13           a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class  
14 Members' Private Information;

15           b. Failing to adequately monitor the security of their networks and systems;

16           c. Failure to periodically ensure that their network system had plans in place to maintain  
17 reasonable data security safeguards;  
18

19           d. Allowing unauthorized access to Class Members' Private Information;

20           e. Failing to detect in a timely manner that Class Members' Private Information had been  
21 compromised;

22           f. Failing to timely notify Class Members about the cyber-attack so that they could take  
23 appropriate steps to mitigate the potential for identity theft and other damages; and  
24

25           g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and  
26 data breach.

27           133. It was foreseeable that Defendant's failure to use reasonable measures to protect Class  
28 Members' Private Information would result in injury to Class Members. Further, the breach of security

1 was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the  
2 financial services industry.

3 134. It was, therefore, foreseeable that the failure to adequately safeguard Class Members'  
4 Private Information would result in one or more types of injuries to Class Members.  
5

6 135. Plaintiff and Class Members are entitled to compensatory and consequential damages  
7 suffered as a result of the cyber-attack and data breach.

8 136. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i)  
9 strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those  
10 systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class  
11 Members.  
12

13 **COUNT II**  
14 **BREACH OF IMPLIED CONTRACT**  
15 **(On Behalf of Plaintiff and All Class Members)**

16 137. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations  
17 contained in paragraphs 1 through 125.

18 138. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into  
19 implied contracts for the Defendant to implement data security adequate to safeguard and protect the  
20 privacy of Plaintiff's and Class Members' Private Information.

21 139. When Plaintiff and Class Members provided their Private Information to Defendant in  
22 exchange for Defendant's services and/or products, they entered into implied contracts with Defendant  
23 pursuant to which Defendant agreed to reasonably protect such information.  
24

25 140. Defendant solicited and invited Class Members to provide their Private Information as part  
26 of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and  
27 provided their Private Information to Defendant.  
28

1           141. In entering into such implied contracts, Plaintiff and Class Members reasonably believed  
2 and expected that Defendant's data security practices complied with relevant laws and regulations and  
3 were consistent with industry standards.

4           142. Class Members who paid money to Defendant reasonably believed and expected that  
5 Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.  
6

7           143. The protection of Plaintiff's and Class Members' Private Information was a material aspect  
8 of the implied contracts between Defendant and its customers, including Plaintiff and Class Members.

9           144. On information and belief, the implied contracts – contracts that include the contractual  
10 obligations to maintain the privacy of Plaintiff's and Class Members' Private Information—are also  
11 acknowledged, memorialized, and embodied in multiple documents, including (among other documents)  
12 Defendant's applicable privacy policy.  
13

14           145. Defendant's express representations, including, but not limited to, the express  
15 representations found in its applicable privacy policy, memorialize and embody the implied contractual  
16 obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy  
17 of Plaintiff's and Class Members' Private Information.  
18

19           146. Plaintiff and Class Members would not have entrusted their Private Information to  
20 Defendant and entered into these implied contracts with Defendant without an understanding that their  
21 Private Information would be safeguarded and protected, or entrusted their Private Information to  
22 Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure  
23 that it adopted reasonable data security measures.  
24

25           147. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did  
26 provide their Private Information to Defendant and paid for the services and/or products Defendant  
27 furnished in exchange for, amongst other things, the protection of their Private Information.  
28

1           148. Plaintiff and Class Members performed their obligations under the contract when they paid  
2 for their services and/or products and provided their valuable Private Information.

3           149. Defendant materially breached its contractual obligation to protect the nonpublic Private  
4 Information Defendant gathered when the information was accessed and exfiltrated by unauthorized  
5 personnel as part of the Data Breach.

6           150. Defendant materially breached the terms of the implied contracts. Defendant did not  
7 maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by its  
8 notifications of the cyber-attack to Plaintiff and thousands of Class Members. Specifically, Defendant did  
9 not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA,  
10 or otherwise protect Plaintiff's and the Class Members' Private Information, as set forth above.

11           151. The cyber-attack and Data Breach was a reasonably foreseeable consequence of  
12 Defendant's actions in breach of these contracts.

13           152. As a result of Defendant's failure to fulfill the data security protections promised in these  
14 contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead  
15 received services and/or products that were of a diminished value to that described in the contracts.  
16 Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in the  
17 value of the services and/or products with data security protection they paid for and the services and/or  
18 products they received.

19           153. Had Defendant disclosed that its security was inadequate or that its did not adhere to  
20 industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person  
21 would have purchased services and/or products from Defendant.

22           154. As a direct and proximate result of the cyber-attack/data breach, Plaintiff and Class  
23 Members have been harmed and have presently suffered, and will continue to suffer, actual damages and  
24 injuries, including without limitation the release and disclosure of their Private Information, the loss of  
25  
26  
27  
28

control of their Private Information, the imminent risk of suffering additional damages in the future, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

155. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the cyber-attack/data breach.

156. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**COUNT III**  
**NEGLIGENCE PER SE**  
**(On Behalf of Plaintiff and All Class Members)**

157. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 125.

158. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

159. Plaintiff and Class Members are within the class of persons that the FTCA was intended to protect.

160. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

161. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

1           162. Defendant's failure to comply with applicable laws and regulations constitutes negligence  
2 *per se*.

3           163. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class  
4 Members, Plaintiff and Class Members would not have been injured.

5           164. The injury and harm suffered by Plaintiff and Class Members was the reasonably  
6 foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was  
7 failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to  
8 experience the foreseeable harms associated with the exposure of their Private Information.

9           165. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class  
10 Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in  
11 an amount to be proven at trial.  
12  
13  
14

15                               **COUNT IV**  
16                               **UNJUST ENRICHMENT**  
17                               **(On Behalf of Plaintiff and All Class Members)**

18           166. Plaintiff restates and realleges paragraphs 1 through 125 above as if fully set forth herein,  
19 and pleads this count in the alternative to the breach of contract count (Count II) above.

20           167. Upon information and belief, Defendant funds its data security measures entirely from its  
21 general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

22           168. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members  
23 is to be used to provide a reasonable level of data security, and the amount of the portion of each payment  
24 made that is allocated to data security is known to Defendant.

25           169. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically,  
26 Defendant enriched itself by saving the costs they reasonably should have expended on data security  
27 measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a  
28

1 reasonable level of security that would have prevented the cyber-attack, Defendant instead calculated to  
2 increase their own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective  
3 security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate  
4 result of Defendant's decision to prioritize their own profits over the requisite security.  
5

6 170. Under the principles of equity and good conscience, Defendant should not be permitted to  
7 retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement  
8 appropriate data management and security measures that are mandated by industry standards.

9 171. Defendant acquired the PII through inequitable means in that it failed to disclose the  
10 inadequate security practices previously alleged.

11 172. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would  
12 not have agreed to provide their PII to Defendant.  
13

14 173. Plaintiff and Class Members have no adequate remedy at law.

15 174. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have  
16 suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the  
17 opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-  
18 pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or  
19 unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of  
20 productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach,  
21 including but not limited to efforts spent researching how to prevent, detect, contest, and recover from  
22 identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject  
23 to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate  
24 measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and  
25 money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as  
26 a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.  
27  
28

175. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

176. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of herself and Class Members, request judgment against Defendant and that the Court grant the following:

- A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
  - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
  - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
  - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

- iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;
- v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
- vi. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
- vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- x. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendants' network is compromised, hackers cannot gain access to portions of Defendant's systems;
- xi. requiring Defendant to conduct regular database scanning and securing checks;
- xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xiii. requiring Defendant to routinely and continually conduct internal training and

- 1 education, and on an annual basis to inform internal security personnel how to  
2 identify and contain a breach when it occurs and what to do in response to a breach;  
3  
4 xiv. requiring Defendant to implement a system of tests to assess its respective  
5 employees' knowledge of the education programs discussed in the preceding  
6 subparagraphs, as well as randomly and periodically testing employees' compliance  
7 with Defendant's policies, programs, and systems for protecting personal identifying  
8 information;  
9  
10 xv. requiring Defendant to implement, maintain, regularly review, and revise as  
11 necessary a threat management program designed to appropriately monitor  
12 Defendant's information networks for threats, both internal and external, and assess  
13 whether monitoring tools are appropriately configured, tested, and updated;  
14  
15 xvi. requiring Defendant to meaningfully educate all Class Members about the threats that  
16 they face as a result of the loss of their confidential personal identifying information  
17 to third parties, as well as the steps affected individuals must take to protect  
18 themselves;  
19  
20 xvii. requiring Defendant to implement logging and monitoring programs sufficient to  
21 track traffic to and from Defendant's servers; and for a period of 10 years, appointing  
22 a qualified and independent third party assessor to conduct a SOC 2 Type 2  
23 attestation on an annual basis to evaluate Defendant's compliance with the terms of  
24 the Court's final judgment, to provide such report to the Court and to counsel for the  
25 class, and to report any deficiencies with compliance of the Court's final judgment;  
26  
27 D. For an award of damages, including actual, nominal, statutory, consequential, and  
28 punitive damages, as allowed by law in an amount to be determined;  
E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;  
F. For prejudgment interest on all amounts awarded; and  
G. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff hereby demands that this matter be tried before a jury.

Respectfully Submitted,

DATED: September 12, 2024

/s/ David Hilton Wise

David Hilton Wise, Esq.

Nevada Bar No. 11014

**WISE LAW FIRM, PLC**

421 Court Street

Reno, Nevada 89501

Tel: (775) 329-1766

Fax: (775) 329-2432

Email: [dwise@wiselaw.pro](mailto:dwise@wiselaw.pro)

M. Anderson Berry, Esq.\*

Gregory Haroutunian, Esq.\*

**CLAYEO C. ARNOLD**

**A PROFESSIONAL CORPORATION**

865 Howe Avenue

Sacramento, CA 95825

Telephone: (916) 777-7777

Facsimile: (916) 924-1829

[aberry@justice4you.com](mailto:aberry@justice4you.com)

[gharoutunian@justice4you.com](mailto:gharoutunian@justice4you.com)

*Attorneys for Plaintiff and the Class*

*\*Pro hac vice forthcoming*